

WHAT IS CLAIMED IS:

1. A method for detecting spam in a messaging system comprising:
generating a white list of confirmed message senders, each of said confirmed message
senders having been confirmed as being able to receive messages;
5 sharing the white list among a plurality of spam filters in the messaging system;
 using the white list at a given one of the plurality of spam filters to determine if a
sender of a received message has been previously confirmed, and if so, forwarding the
received message to a recipient without separately confirming the sender.
2. The method of claim 1 wherein the messaging system is an email system
- 10 3. The method of claim 1 wherein the white list is shared with at least two spam
filters.
4. The method of claim 1 wherein if the sender has not been previously
confirmed, sending a confirmation to the sender, verifying a response from the sender, and if
the response is verified, adding the sender to the white list at the given spam filter and
15 sharing the information with other spam filters in the messaging system.
5. The method of claim 1 wherein sharing includes publishing the white list at a
central location.
6. The method of claim 1 wherein using the white list includes checking the
white list maintained at a central location.
- 20 7. The method of claim 1 wherein the if the sender has not been previously
confirmed, the method further including sending a confirmation to sender, verifying a
response from the sender, and if the response is verified, adding the sender to the white list at
a central location that is shared among the plurality of spam filters.

8. A method for identifying a spam message comprising:

Receiving a message at a spam filter in a network that includes a plurality of spam filters;

- 5 Identifying the sender of the message;

Determining if the sender has been previously confirmed as a valid sender including determining if the sender is included in a list of confirmed senders for any spam filter in the network; and

- 10 If so, then forwarding the received message to a recipient without separately confirming the sender.

9. The method of claim 8 wherein the message is an email message.

10. The method of claim 8 wherein the white list is shared with at least two spam filters.

- 15 11. The method of claim 8 further comprising:

determining if the sender has not been previously confirmed and if not confirmed

sending a confirmation to the sender,

verifying a response from the sender, and

if the response is acceptable,

- 20 adding the sender to the white list at the given spam filter and

sharing information with other spam filters in network, the information including information indicating that the sender has been confirmed.

12. The method of claim 11 wherein sharing includes publishing the white list at a central location

13. The method of claim 11 wherein determining includes checking a white list maintained at a central location

14. The method of claim 13 further comprising

if the sender has not been previously confirmed,

5 sending a confirmation to the sender,

verifying a response, and

if the response is acceptable,

adding the sender to the white list shared among the plurality of spam

filters.

10 15. A method for detecting a spammer in a network that includes a plurality of spam filters:

collecting information relating to a sender from a plurality of the spam filters:

determining a trend in the collected information; and

identify a spammer based on the trend.

15 16. The method of claim 15 wherein collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses.

17. The method of claim 15 wherein determining trends includes correlating the messages received by an individual spam filter relating to a same sender.

18. The method of claim 15 wherein identifying includes determining that a
20 sender is a spammer if a number of messages sent to unrelated email addresses in the correlated data exceeds a predetermined threshold.

19. The method of claim 18 wherein the threshold is time dependent.

20. A method for detecting spam in a messaging system comprising:

generating a white list of confirmed message senders and maintaining the white list at a data center:

receiving a message at a spam filter in a network that includes a plurality of spam filters:

5 verifying with the data center that the sender of the message is a confirmed message sender, add if so, forwarding the received message to a recipient without separately confirming the sender.

21. The method of claim 20 wherein the message is an email message.

22. The method of claim 20 further comprising sharing the white list with at least
10 two spam filters in the network.

23. The method of claim 20 further comprising determining if the sender has not been previously confirmed, and if not confirmed then

 sending from the data center a confirmation to the sender,

 verifying a response received at the data sender, and

15 if the response is acceptable,

 adding to the white list a name identifying the sender and

 sharing information identifying the sender as being confirmed with
other spam filters in network

24. A method for identifying a spam message comprising:

20 Receiving a message at a spam filter in a network that includes a plurality of spam filters;

 Identifying the sender of the message;

 Verifying with a data center coupled to a plurality of the spam filters if the sender has been previously confirmed as a valid sender including determining if the sender is included
25 in a list of confirmed senders for any spam filter in the network, said list maintained at the data center;

If the sender has been previously confirmed, forwarding the received message to a recipient without separately confirming the sender.

25. The method of claim 24 wherein the message is an email message.

26. The method of claim 24 wherein the list is shared with at least two spam
5 filters.

27. The method of claim 24 further comprising determining if the sender has not been previously confirmed, and if not confirmed

sending from the data center a confirmation to the sender,

verifying if the response is acceptable, and

10 adding an name identifying the sender to the list maintained at the data center.

28. A method for detecting a spammer in a network that includes a plurality of spam filters:

collecting, using a data center, information relating to a sender from a plurality of the

spam filters:

15 determining a trend in the collected information;

identify a spammer based on the trend, including adding the sender to a list of confirmed spammers maintained by the data center.

29. The method of claim 28 wherein collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses.

20 30. The method of claim 28 wherein determining trends includes correlating messages received by an individual spam filter relating to a same sender.

31. The method of claim 28 wherein identifying includes determining that a sender is a spammer if a number of messages sent to unrelated email addresses in the correlated data exceeds a predetermined threshold.

25 32. The method of claim 31 wherein the threshold is time dependent.

33. A method for filtering spam in a messaging system comprising:
confirming that a message sender can receive;

sharing information indicating that the message sender can receive among a plurality of spam filters in the messaging system;

using said information at a given one of the plurality of spam filters to determine if a message should be allowed without separately determining whether the message sender can receive.

34. The method of claim 33 wherein the message is an email message.

5 35. The method of claim 33 further comprising confirming at a first spam filter in the system that a sender of a message can receive messages.

36. The method of claim 35 further comprising receiving the message at a second spam filter.

10 37. The method of claim 35 further comprising sharing information developed by the first spam filter with one or more other spam filters in the messaging system.

38. The method of claim 37 further comprising sharing the information with a data center, and thereafter allowing access by each of the spam filters in the messaging system to the information.

15 39. The method of claim 33 wherein the information is maintained in a list of confirmed senders.

40. The method of claim 39 wherein the list is shared with a plurality of the spam filters in the messaging system.

20 41. The method of claim 39 wherein the information is maintained in a list which is maintained by a data center accessible by a plurality of spam filters in the messaging system.

42. The method of claim 41 further comprising sharing the list with a plurality of spam filters in the messaging system.

43. The method of claim 42 further comprising maintaining a copy of the list at a plurality of spam filters in the messaging system.

25 44. The method of claim 39 further comprising associating a passcode with one or more of the confirmed senders in the list, and verifying a message received from a sender in the list includes the passcode if specified.

45. The method of claim 44 further comprising triggering an addition of a passcode for a sender in the list upon an occurrence of an predefined event.

46. The method of claim 45 wherein the event includes detection that an email address associated with the sender has been compromised.

47. The method of claim 39 further comprising including a pass code in the list for each confirmed sender and verifying the pass code is included in the message prior to forwarding the message from the sender to a recipient.

48. The method of claim 47 further comprising automatically adding the passcode associated with the sender at a time for transmission of a message from the sender in the messaging system.

49. The method of claim 48 further comprising providing a plug in module for automatically adding the passcode, the plug in module adapted to add the passcode prior to transmission to the messaging system.

50. The method of claim 33 further comprising correlating sender-recipient data at a spam filter in the messaging system and determining data related to how fast a list of recipients grows for a given sender; determining a list of unacceptable senders using the sender-recipient data and the determined data; and sharing the list of unacceptable senders with other spam filters in the messaging system.

51. The method of claim 50 further comprising maintaining a list of recipients for each sender of messages processed by a given spam filter.

52. The method of claim 51 further comprising maintaining the list of recipients for each sender at a data center.

53. A method for processing messages at a spam filter in a messaging system, the messaging system including a plurality of spam filters, the method comprising: receiving a message for processing, the message from an sender for delivery to an intended recipient;

determining if the sender is a confirmed sender, including querying a data center to determine if the sender is included in a list of confirmed senders based on information received from any of the plurality of spam filters in the messaging system, where confirmed senders are senders having a verified capability to receive messages;

if the sender is a confirmed sender, enabling transmission of the message to the intended recipient.

54. A method for processing messages at a spam filter in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

5 receiving a message for processing, the message from a sender for delivery to an intended recipient;

determining if the sender is a confirmed sender, including querying a data center to determine if the sender is included in a list of confirmed senders based on information received from any of the plurality of spam filters in the messaging system, where confirmed
10 senders are senders having a verified capability to receive messages;

if the sender is not a confirmed sender, confirming the sender including sending the sender a notification;

upon receipt of a confirmation from the sender, sharing the sender's confirmed status with the plurality of spam filters in the messaging system including publishing the sender's
15 status to the data center.

55. A method for minimizing spam in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a
20 verified capability to receive messages;

evaluating a list of confirmed senders;

providing a notification to the one spam filter indicating whether the sender's status is confirmed.

56. A method for minimizing spam in a messaging system, the messaging system
25 including a plurality of spam filters, the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a verified capability to receive messages;

evaluating a list of confirmed senders;

30 if the sender is not included in the list of confirmed senders,

confirming the sender including providing a notification to the sender and
upon receipt of a confirmation from the sender, sharing the sender's status with the
other spam filters in the messaging system including adding the sender to the list; and
providing a notification to the one spam filter indicating whether the sender's status is
5 confirmed.

57. The method of claim 56 wherein the step of confirming the sender is
performed by a spam filter.

58. The method of claim 56 wherein the step of confirming the sender is
performed by the requesting spam filter.

10